UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/830,685 | 07/17/2001 | Christophe Clavier | 032326-138 | 9929 |

7590 02/05/2008

JAMES A. LaBARRE
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. BOX 1404
ALEXANDRIA, VA 22313-1404

| EXAMINER | |
|---|---|
| ABYANEH, ALI S | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2137 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 02/05/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/830,685 | CLAVIER ET AL. | |
| | Examiner | Art Unit | |
| | Ali S. Abyaneh | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) 1-8 and 11-15 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-8 and 11-15 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-8 and 11-15 are presented for examination.

2. Claims 1, 2 and 12 are amended.

## Response to Arguments

3. Applicant's amendments/arguments filed on 11-30-2007 have been fully considered but are moot in view of the new ground(s) of rejection.

4. In the claim sheet presented on 11-13-2007, claim 8 has been identified as an amended claim, but the text in the claim does not include any changes to the claim. Applicants are encouraged to review the claim and if the claim is amended show the changes by strike-through (for deleted matter) or underline (for added matter).

## *Claim Rejections - 35 USC § 112*

5. The following is a quotation of the second paragraph 0f 35 U.S.C. 112

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1 and 12 are rejected under 35 U.S.C. 112 second paragraphs for following reasons:

In claim 1, the term "first manipulation means" and " means of instructions" is not defined by the claim, the specification does not provide a

standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

In claim 12, the term "first manipulation means" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-8 and 11-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (US Patent NO.6278783) in view of Luyster (US Patent NO 6,182,216).

**Regarding claim 1**

Kocher explicitly teaches a countermeasure method in an electronic component using a cryptographic algorithm that comprises multiple successive rounds of operation with a secret key, (column 12, lines 18-24), wherein at least one of the said rounds is implemented with a first manipulating means for supplying an output data item from an input data item, (column 6, lines 39-42) and the output data

item is manipulated by means of instructions (column 6, lines 47-49) and wherein at least one other round of said algorithm is implemented with other manipulation means for supplying output data, so that the output data item is unpredictable (column 6, lines 39-53).

Kocher does not explicitly teach said other manipulation means being obtained from said first manipulation means by performing an exclusive OR operation on said first manipulation means with a random value. However, in an analogous art, Luyster teaches other manipulation means being obtained from said first manipulation means by performing an exclusive OR operation on said first manipulation means with a random value (column 6, lines 39-53 and fig 6. block 124).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Kocher to include, other manipulation means being obtained from said first manipulation means by performing an exclusive OR operation on said first manipulation means with a random value. This would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so in order to provide cryptographic systems and methods which are secure and to resist attacks by sophisticated algorithms which detect and take advantage of weak subkeys to determine the keys of the cryptographic system (column 15, lines 27-39).

**Regarding claim 12**

Kocher teaches an electronic security component have a countermeasure against attacks on a secret key cryptography technique in which data is manipulated during multiple successive rounds of a cryptograph algorithm, said component comprising: a program memory having stored therein a first manipulating means that produces an output value from an input value (column 2, lines 35,36) means for generating a random value (column 6, lines 39-53).

Kocher does not explicitly teach means for calculating at least one other manipulating means by combining said first manipulating means with said random value and a processor that executes said algorithm using said first manipulating means during some of said multiple rounds and said other manipulating means during other rounds of said algorithm. However, in an analogous art, Luyster teaches means for calculating at least one other manipulating means by combining said first manipulating means with said random value (column 6, lines 39-53 and fig 6. block 124) and a processor that executes said algorithm using said first manipulating means during some of said multiple rounds and said other manipulating means during other rounds of said algorithm (column 15-line 63-collumn 16, line11).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Kocher to include means for calculating at least one other manipulating means by combining said first

manipulating means with said random value and a processor that executes said algorithm using said first manipulating means during some of said multiple rounds and said other manipulating means during other rounds of said algorithm.

This would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so in order to provide cryptographic systems and methods which are secure and to resist attacks by sophisticated algorithms which detect and take advantage of weak subkeys to determine the keys of the cryptographic system (column 15, lines 27-39).

**Regarding claim 2 and claim 5**

Kocher furthermore teaches wherein said algorithm comprises sixteen calculation rounds, each round using manipulation means for supplying an output data item from an input data item, the output data item being manipulated by instruction in the first three and the last three rounds, and wherein said method includes the steps of forming a first group comprising at least the first three rounds and another group comprising at least the last three rounds, and implementing the first group and the last group with an execution sequence using the other manipulation means in at least some (see column 9, line 1-column 10, line 38).

**Regarding claim 3 and claim 4**

Luyster furthermore teaches a countermeasure method wherein four groups of successive rounds are formed and said execution sequence is applied at least to the first group and to the last group, wherein the sequence is executed in each of the groups (see column 7, lines 16-51).

**Regarding claim 6**

Kocher furthermore teaches a countermeasure method wherein each execution of the algorithm includes the steps of drawing a random value and calculating said other manipulation means. (column 6, Lines 39-53).

**Regarding Claim 7**

Kocher furthermore teaches a method wherein said manipulation means are tables of constants. (column 7, Lines 16-65).

**Regarding claim 8**

Kocher furthermore teaches a method wherein said manipulation means are used in combination with an additional exclusive OR operation with a value based upon the random value. (column 6, lines 39-53).

**Regarding Claim 11**

Kocher furthermore teaches wherein said random value is

derived from one or both of the input and output data of said first manipulation means. (column 6, Lines 39-53).

**Regarding claim 13**

Kocher furthermore teaches wherein said first and said other manipulating means each comprise a table of constants. (column 7, lines 16-65).

**Regarding claim 14**

Kocher furthermore teaches wherein said cryptography technique comprises a DES algorithm that is executed in multiple rounds (column 9, lines 1-67, column 10, lines 1-39 and column 11,
lines 41-55).

**Regarding claim 15**

Kocher furthermore teaches the electronic security component of claim 12, wherein said component is a chip card. (column 14, lines 1-8).

**Conclusion**

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300 Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/31/08

Ali Abyaneh AA
Patent Examiner
Art Unit 2137
01/25/08